Journal of the Korea Academia-Industrial cooperation Society
Vol. 17, No. 9 pp. 308-313, 2016

http://dx.doi.org/10.5762/KAIS.2016.17.9.308
ISSN 1975-4701 / eISSN 2288-4688

안전중시 시스템의 모델기반 설계에서 메타모델을 활용한 기능 고장의 탐지 및 안전 요구사항 검증

김영현, 이재천*
아주대학교 시스템공학과

Detection of Functional Failure and Verification of Safety Requirements Using Meta-Models in the Model-Based Design of Safety-Critical Systems

Young-Hyun Kim, Jae-Chon Lee*
Dept. of Systems Engineering, Ajou University

요 약 사용자의 요구사항 증대와 기술의 발전으로 인해 현대 시스템은 계속해서 복잡해지고 있어 시스템 설계 오류 및 고장 등으로 인한 시스템 운용 중의 사고도 빈번해지고 있다. 특히 사고로 인한 인적 및 물적 피해가 심각할 수 있는 시스템을 안전중시 시스템이라고 부른다. 이러한 시스템에 대해서는 안전성을 확보하기 위한 특별한 노력이 필요한데 이에 부응하여 본 논문에서는 개발 초기 단계부터 안전성을 반영하면서 시스템 설계를 수행할 수 있는 방법을 연구하였다. 특히 안전 메타모델을 활용해서 기능의 고장 탐지를 수행할 수 있는 시스템 설계 방법을 제시하였다. 구체적으로 국제 안전 표준들을 참고하여 안전 데이터를 추출하고, 시스템 모델링 표준 언어인 SysML을 이용하여 안전 데이터 메타모델을 생성한 후, 시스템 설계에서 안전 데이터 메타모델을 효과적으로 활용하는 모델 기반 안전 시스템 설계 방법을 제시하였고, 이를 기반으로 안전요구사항 생성 및 시뮬레이션 방법에 관하여 논의하였다. 마지막으로 사례연구로서 자동차 시스템 설계에서 SysML 기반 모델링 및 시뮬레이션을 통해 기능 고장의 탐지나 안전 요구사항의 검증이 가능한 것을 보여 주었다. 본 연구에서 안전 데이터에 대한 메타모델의 활용을 통해 안전 데이터 및 정보의 구성 및 관리를 효율적으로 수행할 수 있는 것과, 메타모델 기반 시스템 설계와 시뮬레이션을 활용하여 설계 오류를 줄임으로써 요구사항에 맞는 시스템 설계를 할 수 있음을 제시하였다.

Abstract Modern systems have become more and more complex due to the ever-increasing user requirements and rapid advance of technology. As such, the frequency of accidents due to system design errors or failure has been increasing. When the damage incurred by accidents to human beings or property is serious, the underlying systems are referred to as safety-critical systems. The development of such systems requires special efforts to ensure the safety of the human beings operating them. To cope with such a requirement, in this paper an approach is employed in which we consider safety starting from the conceptual design phase of the systems. Specifically, a systems design method that can detect functional failure is proposed by utilizing meta-models and M&S methods. To accomplish this, the safety design data from international safety standards are first extracted and also a meta-model is generated using SysML (systems modeling language). Then, a SysML-based system design method is proposed based on the use of the developed meta-model. We also discuss how the safety requirements can be created and verified using a simulation method. Finally, through a case study in automotive design, it is demonstrated that the detection of a functional failure and the verification of a safety requirement can be accomplished using the SysML-based M&S method. This study indicates that the use of meta-models can be useful for collecting and managing safety data and that the meta-model based M&S method can make it possible to satisfy the system requirements by reducing the design errors.

Keywords : Model-Based Systems Engineering(MBSE), Meta-Model, Safety, Simulation, SysML

본 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임.
(No. NRF-2015R1D1A1A01056730)
*Corresponding Author : Jae-Chon Lee(Ajou Univ.)
Tel: +82-31-219-3941 email: jaelee@ajou.ac.kr
Received July 27, 2016 Revised (1st August 16, 2016, 2nd August 19, 2016)
Accepted September 9, 2016 Published September 30, 2016

1. 서론

현대 사회에서 안전이 매우 중요한 문제로 부상하여 각 산업분야에서는 안전관련 표준을 제정하고 있다. 안전 표준들의 공통적인 특징은 시스템공학에서 제시하고 있는 시스템 개발 전 수명주기 관점을 기반으로 안전성 확보를 위한 안전 활동 및 방법을 제시하고 있다는 점이다[1].

시스템을 체계적으로 설계하기 위한 방법으로 MBSE(Model Based System Engineering)가 하나의 추세로 자리 잡아가고 있는데, 시스템 개발에서의 개념 및 설계 산출물 들을 모델로 표현함으로써 의사소통을 원활하게 할 수 있으며 설계 결과를 좀 더 명확하게 할 수 있다[2,3]. 시스템 모델링언어로서는 표준 언어인 SysML을 많이 활용하고 있다[4]. SysML은 안전성을 확보하려는 시스템 설계에서도 활용되고 있으며, 메타모델이나 시뮬레이션으로까지 확장해서도 활용하고 있다[3,5].

특히, 메타모델에 관한 기존 연구들은 정의나 구성에 초점이 맞춰져 있는데, 본 논문에서는 메타모델을 활용한 안전 시스템 설계에 초점을 맞추려고 한다. 구체적으로, 안전 데이터 메타모델을 SysML로 생성하고 SysML 기반 안전 시스템 설계에 활용하는 방법을 연구한다. 게다가 시스템의 고장 모드 탐지 및 요구사항 검증을 위한 SysML기반 시뮬레이션 기법도 제시한다. 연구 결과들을 자동차 시스템의 안전설계에 적용함으로써 안전 요구사항으로부터 안전 시스템을 체계적으로 설계하는 방법을 평가한다.

본 논문의 구성은 제1장 서론에 이어 제2장에서는 메타모델에 관한 선행연구 분석을 하고, 제3장에서는 메타모델을 활용한 SysML기반 안전 시스템 설계에 대해 기술하였다. 제4장에서는 제3장에서 제시한 방법을 자동차 시스템 설계 사례에 적용하였다. 마지막으로 제5장에서는 결론을 기술하였다.

2. 메타모델에 관한 선행연구 분석

2.1 메타모델의 정의 및 개념

시스템이 복잡해짐에 따라 모델기반 시스템 설계에서는 설계 데이터들을 구성하고 관리하기 위한 방안으로 메타모델이 제시되고 있다[5]. 메타모델은 모델을 다시 모델로 표현하는 것으로써 공통적인 특징을 가지고 있는 모델이나 모델 요소들을 다시 하나의 모델로 표현하는 것이다[4]. 메타모델의 가장 큰 장점으로는 설계에 대한 데이터를 효율적으로 구성하거나 관리할 수 있을 뿐만 아니라 재사용 또한 가능하다. SysML에서는 이런 메타모델을 표현하기 위해서 프로파일 모델을 제공하고 있다.

메타모델에 대한 선행연구를 보면 다양하게 활용되는 모습을 볼 수 있다. Pfister는 시스템공학기반의 설계에서 기능적 측면과 구조적 측면의 패턴을 분석해서 메타모델로 나타냈다[6]. Piriou는 공학프로세스에서의 개념, 관계, 입출력 데이터들의 정보와 함께 시스템 안전을 위한 중복 설계 및 고장모드에 대한 부분을 메타모델에 추가했다[7]. Vara는 안전 관련 데이터 및 정보를 관리하기 위한 메타모델을 제시했다[5]. 국내 연구사례로는 소프트웨어 개발에서 프레임워크를 제시하거나 모바일 웹서비스 구성을 위해 메타모델을 활용하기도 했다[8,9].

2.2 안전 시스템 모델링에서의 메타모델

Vara[5]가 안전 표준 37개를 참고하여 제시한 안전 표준 데이터 메타모델은 Requirement, Activity, Role, Artefact, Technique, Criticality Kind, Applicability Kind로 구성되어 있으며 안전 시스템 모델링에서 활용될 수 있다. Requirement는 안전 요구사항을 나타내고, Activity는 안전 설계 활동 요소를 나타낸다. Role은 Activity를 하게 될 구성원 정보를, Artefact는 설계 활동에서 관리해야 하는 데이터 요소를 나타낸다. Technique는 앞에서 제시한 Activity 수행과 Artefact 생산에 대해 구체적으로 필요한 기술 또는 방법을 나타낸다. Criticality Kind는 시스템 또는 구성품의 리스크 감소를 위한 기준을, Applicability Kind는 받아들일 수 있는 리스크 수준이 되었는지를 나타내고 있다.

2.3 연구 목표 및 수행방법

메타모델에 대한 선행연구들은 메타모델을 정의하고 모델로 표현하는 것을 중심으로 진행한 연구가 대부분이다. 그렇기 때문에 본 논문에서는 메타모델을 활용한 모델기반 설계를 통해서 안전 요구사항에 맞는 시스템 설계를 체계적으로 수행하고 검증하는 것을 연구 목표로 설정하였다. 연구 목표를 달성하기 위해 먼저 안전 데이터 메타모델을 SysML 프로파일 모델로 모델링한다. 그리고 안전 요구사항으로부터 메타모델을 활용한 SysML

기반 설계를 수행한다. 또한 생성된 SysML 모델들로 시뮬레이션 수행을 통해 기능의 고장모드 탐지 및 안전 요구사항 검증에 대해 연구한다.

3. 안전 데이터 메타모델을 활용한 SysML기반 안전 시스템 설계

3.1 SysML기반 안전 메타모델의 생성

SysML의 프로파일 모델은 첫 번째로 Package 모델요소에 SysML의 Block Definition Diagram(BDD)을 생성해야 하는데 이 때 Package 모델요소를 Profile로 변경해야 한다. 두 번째로 Stereotype은 Profile 모델 요소 없이는 생성될 수 없기 때문에 BDD에 Profile 모델 요소를 생성한다. 세 번째로 Profile 안에 Stereotype을 생성하고, 네 번째로 Stereotype에 Meta-class를 정의해서 Stereotype이 가지고 있는 속성을 나타낸다. 마지막으로 생성된 Stereotype들의 관계를 설정하면 메타모델의 구성이 모델로 표현된다. 이러한 절차는 Fig. 1에서 확인할 수 있으며 이 절차에 따라 2장에서 분석한 안전 데이터 메타모델을 메타모델로 표현할 것이다.

먼저 Safety Profile BDD를 생성한 다음 Safety Profile을 모델링하고 안전 데이터 메타모델을 관리할 SAF(Safety Assurance Framework)와 2장에서 제시한 안전 데이터 7가지 구성요소를 Stereotype으로 모델링한다.

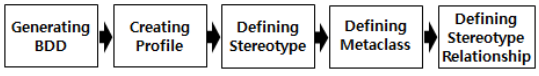

Fig. 1. Procedure for generating meta-models using SysML

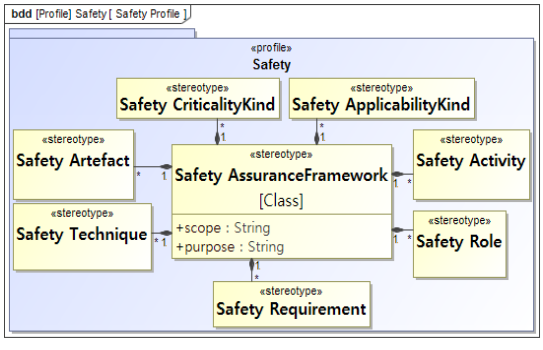

Fig. 2. Meta-model for safety data

다음으로 SAF에 Class를 Meta-class로 설정한다. 마지막으로 SAF에 안전 데이터 요소들이 포함되게 연결하면 안전 데이터 메타모델이 구성된다. 이렇게 구성된 안전 데이터 메타모델을 Fig. 2에 나타내었는데, 안전 데이터 메타모델 사이의 관계까지 모델링되어 있는 것을 확인할 수 있다.

3.2 안전 데이터 메타모델을 활용한 대상 시스템의 안전 설계 모델링

모델기반 안전 설계는 크게 3가지 단계로 구성된다. 처음에는 안전 요구사항을 식별하고 Requirement Diagram으로 나타낸다. 그 다음 안전 요구사항에 맞는 안전 기능 아키텍처를 거동 다이어그램(Behavior Diagram)으로 생성하고 마지막으로 안전 기능을 수행할 물리 아키텍처를 구조 다이어그램(Structure Diagram)으로 정의해야 한다. 추가적으로 Parametric Diagram을 활용한 시뮬레이션을 구성할 수 있다. 이러한 절차를 Fig. 3에 요약하였다.

구체적으로, 안전 요구사항을 모델링하기 이전에 안전 요구사항을 식별하고 안전 데이터 메타모델에서 제시한 Safety Requirement를 요구사항에 Stereotype으로 모델링하게 된다. 이렇게 모델링 된 안전 요구사항은 일반 요구사항과 구별되기 때문에 식별하기가 쉽고 이를 바탕으로 모델기반 설계 또한 체계적으로 할 수 있다. 안전 요구사항에서 분해된 안전 기능에 대한 요구사항을 거동 다이어그램을 이용해서 표현할 때 안전 데이터 메타모델에서 제시한 Safety Activity Stereotype을 활용할 수 있고 이 때 발생되는 구체적인 데이터 요소를 Safety Artefact Stereotype을 이용해서 표현할 수 있다. 즉, 안전 기능은 기능의 흐름과 기능에서 사용될 데이터 요소들을 함께 표현하는 것임을 알 수 있다. 그리고 안전기능을 수행할 물리요소를 구조 다이어그램으로 나타내는데, 상위 수준에서 안전기능을 수행하는 물리요소에는 Safety Technique를, 하위 수준의 물리요소에는 리스크에 기준

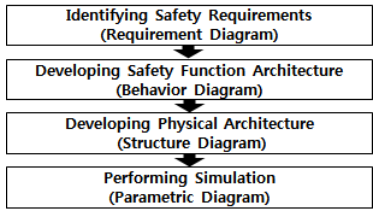

Fig. 3. Procedure for safety design using models

이 되는 Applicability Kind와, Criticality Kind를 적용할 수 있다.

3.3 시뮬레이션을 통한 요구사항 검증

SysML기반으로 할 수 있는 시뮬레이션은 2가지 종류가 있다. 하나는 거동 시뮬레이션으로서 시간의 변화에 따라서 거동의 흐름을 시뮬레이션으로 나타내는 것이다. 이런 거동 시뮬레이션을 통해서 시스템의 논리적 검증을 할 수 있다. 또 다른 한 가지 방법은 수식을 활용한 시뮬레이션이다. SysML에서는 UML에 존재하지 않는 Parametric Diagram을 지원하고 있는데 이것을 활용하여 수식을 사용한 시뮬레이션을 할 수 있어서 수학적 검증에 활용할 수 있다.

안전 요구사항을 바탕으로 설계된 모델을 검증하기 위해서 거동 시뮬레이션의 조건을 설정해서 실제 거동과 유사하게 표현하고 요구사항에 맞는 시스템 설계를 했는지 논리적으로 검증할 수 있다. 게다가 수식 시뮬레이션의 수식과 값들을 모델링하고 그 사이의 관계를 정의함으로서 안전 요구사항에 맞는 값을 도출했는지 수학적으로 검증할 수 있다.

4. 안전 데이터 메타모델을 활용한 SysML기반 자동차 안전 시스템 설계

4.1 메타모델을 활용한 SysML기반 자동차 시스템 설계

시스템의 체계적인 설계는 요구사항으로부터 시작된다. 자동차 엔진에 대한 안전 기능 요구 사항으로는 자동차 엔진 토크에 문제가 발생할 경우 운전자에게 알려줘야 하는 것이고, 성능 요구사항으로는 엔진에 이상이 발생하지 않기 위해 자동차 엔진에서 발생되는 최소 토크양을 나타내고 있다[10]. 자동차 엔진 토크에 대한 안전 요구사항을 Fig. 4에서 SysML Requirement Diagram을 활용하여 표현하고 있다. 안전 데이터 메타모델의 Safety Requirement를 요구사항 모델요소에 정의하고 있는 것도 확인할 수 있다.

자동차의 동력 전달 기능은 토크가 발생되고 토크를 증폭시킨 후에 토크를 분배하고 실제 이동하는 힘으로 전달하기에 이른다. 안전 기능 요구사항을 바탕으로 토크가 증폭된 후 토크의 양에 문제가 발생했다면 토크 이

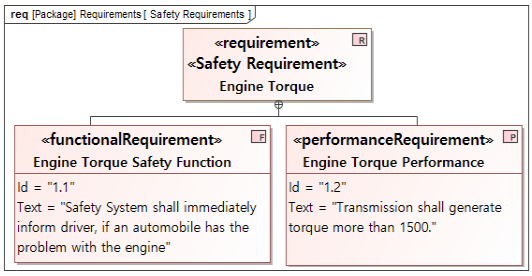

Fig. 4. Requirement diagram for “Engine Torque”

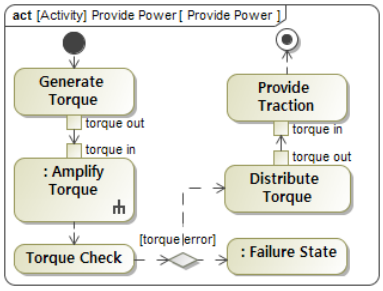

Fig. 5. Activity diagram for “Provide Power”

상(torque error)라는 메시지와 함께 자동차가 고장모드 상태로 변경되는 것을 안전 기능 아키텍처로 나타낸 것이 Fig. 5이다.

자동차 시스템을 상위 수준에서 보면 자동차는 Body, Power Train 등으로 구성되어 있다. 가장 상위에서 자동차 시스템을 나타내고 있는 Vehicle Block과 그 구성 요소들을 Composit Path로 연결한 것을 확인할 수 있는데, 이것은 화학적 결합을 나타내며 하위 구성 요소들의 집합으로 자동차가 구성되어 있는 것을 보여준다. 게다가 Safety System Block에는 안전 데이터 메타모델의 Safety Technique가 적용되어 있다는 것을 확인할 수 있다. 자동차에 대한 물리 아키텍처는 Fig. 6에서 BDD를 통해 확인할 수 있다.

시스템 공학에서 제시하고 있는 복잡한 시스템을 설계하기 위한 방법 중에 하나가 시스템을 분해하는 방법이다. Fig. 6에서 모델링 된 자동차 서브시스템 중에 자동차의 동력을 전달하는 장치인 Power Train을 더 상세한 구조로 모델링을 했다[10]. Power Train은 자동차의 입력을 나타낼 수 있는 값들과, 토크를 발생시키는 엔진, 토크를 증폭시키는 트랜스미션, 바퀴로 동력을 전달하는 디퍼렌셜 기어, 동력을 받고 실제로 움직이게 되는 바퀴로 구성이 되어 있는데 이는 Fig. 7에서 확인할 수 있다.

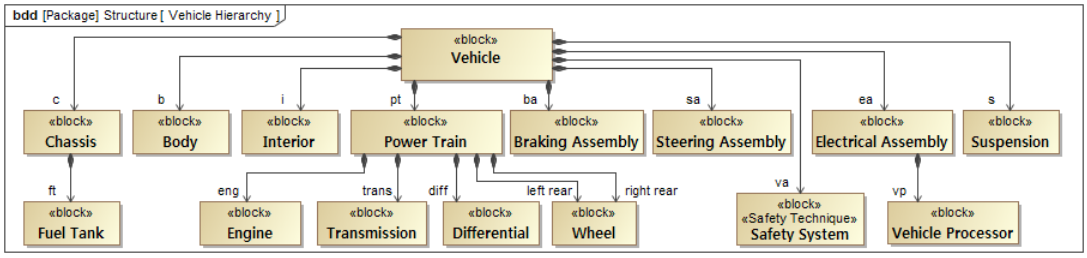

Fig. 6. Block definition diagram for “Vehicle top-level hierarchy"

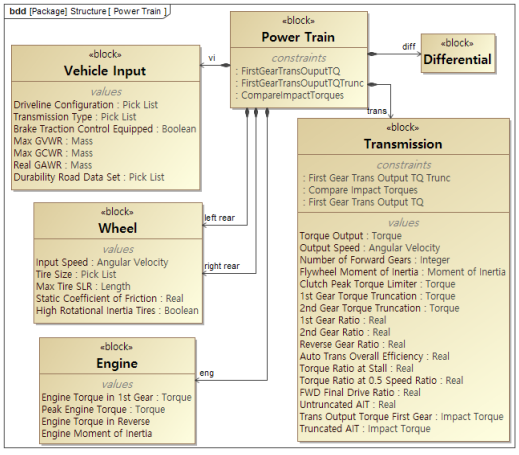

Fig. 7. Block definition diagram for “Power Train”

Power Train을 구성하고 있는 Block들은 Value와 Constraint를 가지고 있는 것을 확인할 수 있다. Constraint에는 사용하게 되는 수식을 나타내며, Value는 해당 Block에서 사용하게 되는 값을 표현한 것이다. 트랜스미션의 Value와 Constraint를 통해 토크의 양을 계산할 수 있다.

4.2 시뮬레이션을 통한 안전 요구사항 검증

거동 시뮬레이션을 통해 모델링에 따른 거동 흐름을 애니메이션으로 확인 할 수 있다. 트랜스미션에서 토크 양을 확인했을 때 문제가 감지되면 토크 이상 메시지를 받고 자동차가 고장상태로 들어간 상황에 대한 시뮬레이션 결과를 Fig. 8에서 확인할 수 있다.

Fig. 9에서는 Parametric Diagram을 활용해서 시뮬레이션을 하고 그 결과를 그래프로 나타낸 것이다. 세로축은 토크의 양을 가로축은 엔진에서 문제가 발생했을 때 토크의 양이 감소되는 정도를 나타냈다. 빨간색 선은 GTDI 3.0 엔진, 파란색 선은 GTDI 2.0 엔진, 초록색 선은 PF/DI 3.3 엔진의 토크의 양을 보여주고 있다[10]. 그래프에서 보면 기어가 1단인 경우에는 엔진에서 발생되는 토크의 최소 양이 1500을 넘어야 한다. 엔진 1 파란색 선은 토크 발생량이 70%이하로 떨어지면 문제가 발생하는 것을, 엔진 3 초록색 선은 75%이하로 떨어지면 문제가 발생하는 것을 확인할 수 있다. 엔진 2 빨간색 선은 엔진의 토크 발생량이 80%까지 떨어져도 최대 토크 양에는 문제가 없는 것을 확인 할 수 있으며 45%이하로 떨어지면 문제가 발생하는 것을 확인 할 수 있다.

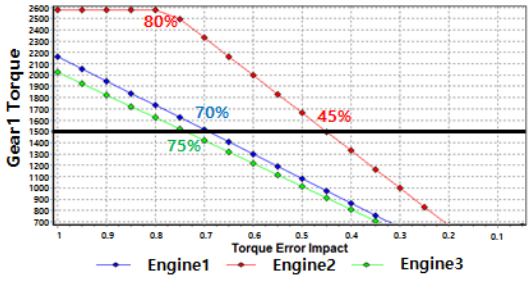

Fig. 9. Performance simulation for “Engine Torque”

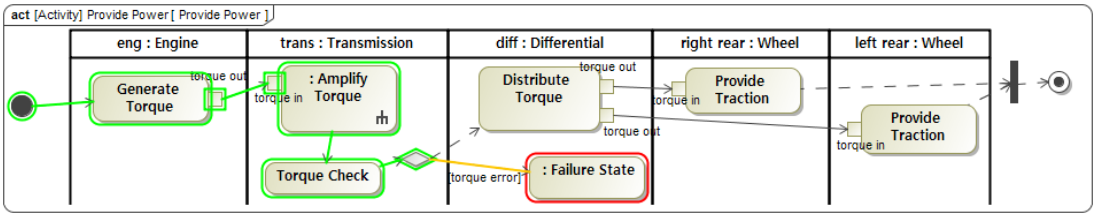

Fig. 8. Behavior simulation of safety function

5. 결론

본 연구에서는 모델기반 설계방법을 보다 효율적이고 체계적으로 사용하기 위한 방안으로 메타모델을 활용하는 방법을 제시하였다. 특히, 안전이 중요시되고 있는 만큼 안전 데이터 메타모델을 생성하고 활용하기 위해서 자동차 엔진 시스템의 모델기반 설계에 적용해보았다. 그 결과 모델기반설계에서 안전 요소의 구성 및 식별을 확인 할 수 있었으며 모델 기반의 시뮬레이션을 통해 안전 요구사항을 검증할 수 있는 것을 확인할 수 있었다.

기존 모델기반 설계 방법에서 메타모델을 활용하면 다양한 장점이 있는데 그 첫 번째로 모델기반 설계에 시작하기 전에 시스템 설계에서 필요한 요소들을 미리 확인할 수 있고, 두 번째로 시스템 프로세스에 단계별로 알맞게 적용을 해서 추적성 확보 및 효율적인 설계 데이터를 구성을 할 수 있다. 세 번째로 설계가 진행됨에 따라 복잡성이 증가해도 필요한 요소를 식별하는데 문제가 없다. 마지막으로 한번 정의가 잘 된 메타모델을 다른 모델기반 설계에서도 재사용을 할 수 있다는 점이다.

본 논문에서는 안전 데이터에 관한 메타모델만 정의했지만 향후에는 일반적인 시스템 설계에 대한 메타모델이나 특정 도메인에도 메타모델을 적용해 범위를 확장시켜 사용할 수 있을 것으로 예상된다.

References

[1] Functional safety of electrical / electronic / programmable electronic safety-related systems, IEC Standard, 61508, 2010.

[2] A. Baouya, D. Bennouar, O. A. Mohamed, and S. Ouchani, "A quantitative verification framework of SysML activity diagrams under time constraints," Expert Systems with Applications, vol. 42, no. 21, pp. 7493-7510, 11, 2015.

[3] A. Garro, J. Groß, M. R. gen. Richter, and A. Tundis, "Reliability analysis of an Attitude Determination and Control System (ADCS) through the RAMSAS method," Journal of Computational Science, vol. 5, no. 3, pp. 439-449, 5, 2014.

[4] S. Friedenthal, A. Moore and R. Steiner, A Practical Guide To SysML, Elsevier, 2015.

[5] J. L. de la Vara, A. Ruiz, K. Attwood, H. Espinoza, R. K. Panesar-Walawege, A. Lopez, I. del Rio, and T. Kelly, "Model-based specification of safety compliance needs for critical systems: A holistic generic meta-model," Information and Software Technology, vol. 72, pp. 16-30, 4, 2016.

[6] F. Pfister, V. Chapurlat, M. Huchard, C. Nebut, and J. “A proposed meta-model for formalizing systems engineering knowledge, based on functional architectural patterns," Systems Engineering, vol. 15, no. 3, pp. 321-332, 2012.
DOI: http://dx.doi.org/10.1002/sys.21204

[7] P. Y. Piriou, J. M. Faure, and G. Deleuze, "A Meta-Model to Support the Integration of Dependability Concerns Into Systems Engineering Processes: An Example From Power Production," IEEE Systems Journal, vol. 10, no. 1, pp. 15-24, 2016.
DOI: http://dx.doi.org/10.1109/JSYST.2014.2328663

[8] E. S. Cho, "Design of Methodology Framework based on Meta-Model", Journal of the Korea Academia-Industrial cooperation Society, vol. 16, no. 10, pp. 6969-6976, Aug. 2015.
DOI: http://dx.doi.org/10.5762/KAIS.2015.16.10.6969

[9] C. J. Kim, C. Y. Song, "A MetaModel for Dynamic Mobile Web Service", Journal of the Korea Academia-Industrial cooperation Society, vol. 16, no. 10, pp. 6458-6465, Aug. 2015.
DOI: http://dx.doi.org/10.5762/KAIS.2015.16.10.6458

[10] R. Kraus, "Application of model based system engineering (MBSE) principles to an automotive driveline sub-system architecture," M.S thesis, Science in Product Development, Detroit Mercy, Detroit, MI 2016.

김 영 현(Young-Hyun Kim) **[준회원]**

- 2012년 2월 : 가천대학교 컴퓨터미디어학과 (공학사)
- 2015년 3월 ~ 현재 : 아주대학교 시스템공학과 (석사과정)

<관심분야>
시스템공학, 모델기반 시스템공학, 시스템 안전, M&S

이 재 천(Jae-Chon Lee) **[정회원]**

- 1984년 9월 ~ 1985년 9월 : 미국 MIT Post Doc 연구원
- 1985년 10월 ~ 1986년 10월 : 미국 Univ. of California 방문연구원
- 1990년 2월 ~ 1991년 2월 : 캐나다 Univ. of Victoria(Victoria, BC) 방문교수
- 2002년 3월 ~ 2003년 2월 : 미국 Stanford Univ. 방문교수
- 1994년 9월 ~ 현재 : 아주대학교 시스템공학과 정교수

<관심분야>
시스템공학 (SE), Model-Based SE (MBSE), Systems Safety, Systems T&E, Modeling & Simulation